Submission to Office of the Privacy Commissioner of Canada: Draft Guidance for Biometric Processing

BC Freedom of Information and Privacy Association (FIPA)

Authored by BC FIPA Legal Researchers:

Noah Escandor
Jerika Caduhada
Gage Smith

2024.01.10

Freedom of Information and Privacy Association

Territorial Acknowledgement

FIPA acknowledges with respect the Indigenous Peoples on whose traditional territory we conduct activities. We acknowledge the insight and knowledge of Elders past, present, and emergent and their relationship to this land and these issues. While striving to increase privacy protection and access to information for everyone, we recognize that colonization and associated attitudes, policies and institutions have significantly changed Indigenous Peoples' relationship with this land. For many years, those same things served to exclude Indigenous Peoples from the privacy protection and access to information afforded to others. FIPA is committed to redressing those historic and continued barriers.

About FIPA

The BC Freedom of Information and Privacy Association (FIPA) is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. While we are based in BC, our membership extends across Canada and we regularly partner with organizations throughout the country.

Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform. We are one of very few public interest groups in Canada devoted solely to the advancement of freedom of information and privacy rights.

Institutional Funders

The BC Freedom of Information and Privacy Association thanks the Law Foundation of BC and all our contributors including donors, funders, and volunteers for their ongoing support of our advocacy, programs, projects, and activities. We also acknowledge the financial support of the Province of British Columbia (Gaming Policy and Enforcement Branch).

Table of Contents

Introduction

The overarching purpose of BC FIPA's submission is to recommend that the Office of the Privacy Commissioner of Canada (OPC) amend both draft guidance documents on biometric processing to account for the interests and considerations of marginalized populations.[1]

Our assessment showed that the current guidance documents fail to adequately call for private organizations and public institutions to consider the risks of biometric processing for marginalized people, be they employees, clients, or consumers. In the privacy context, discrimination primarily deprives an individual of their right to self-determination, which is exacerbated for marginalized populations.[2] In their interactions with public institutions and private organizations, those who experience marginalization will more commonly sacrifice their personal information when navigating institutions such as the medical or public welfare systems, than those who are not marginalized.[3] Even if discrimination against marginalized groups is unintentional, existing structural discrimination must be acknowledged by both public and private organizations. Without considering the perspectives of those who are marginalized, public and private organizations are more likely to neglect the protection of those who are the most vulnerable in society, especially when it comes to biometric processing.

Privacy offices across Canada, including the OPC, have affirmed the importance of considering marginalized perspectives as evidenced in their joint resolutions. For public bodies, as per the joint resolution *Reinforcing Privacy and Access to Information Rights During and After a Pandemic* (2021), it is critically important to ensure the distribution of privacy risks and benefits amongst society takes into consideration marginalized populations. For organizations and their employees, as noted in the joint resolution *Protecting Employee Privacy in the Modern Workplace* (2023) without an effective legislative and administrative regime, the privacy rights of employees are left vulnerable and open to exploitation. This exploitation stems from the inherent power imbalance existing between employers and employees, which is heightened in the context of marginalized employees.

BC FIPA's legal research staff, who have authored this submission, is entirely composed of racialized law students. In our relatively short time

[1] For this submission, we define marginalized as those, individuals or groups, who have historically been directly or indirectly discriminated against.
[2] Stephen Kabera Karanja, "Privacy and Protection of Marginalized Social Groups" (2008) 2:3 Studies in Ethics, L, and Tech at 6.
[3] Michelle Gilman & Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization" (2018) 42 NYU Rev L & Soc Change 253 at 253.

working in the field of privacy and access law, we have noticed a disproportionately low amount of consideration for marginalized groups. The rights and interests of marginalized populations are important to our organization, and this is reflected in our current and completed projects.

For this submission, we will be focusing particularly on the perspectives of racialized, LGBTQ2SIA+, and Indigenous people. This is not a comprehensive representation; there are also many populations that should be considered, such as the unhoused, religious groups, seniors, and those living with disabilities. It is important to recognize the intersectionality and lived experience of all marginalized groups.

Racialized Considerations

Whether the discrimination originates in technological or human bias, racialized people have historically experienced discrimination through biometric processing.[4]

The OPC has been demonstrably concerned about the accuracy of facial recognition technology and the possible associated risks for racialized people, as evidenced in the *Joint investigation of Clearview AI, Inc.* by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta (2021). Further, the joint investigation document cites research reports which found that racialized people, especially racialized women, have a higher incidence of false positives or misidentifications when subjected to facial recognition technology analyses. Not only are racialized people more likely to be inaccurately assessed by biometrics which may lead to discrimination, racialized people may generally interact more with biometric processing than others. For example, racialized people may work in low wage sectors that commonly erode workers' privacy rights through invasive biometric processing.[5]

One consistent theme in our research was that, in Canada, a collectivistic approach to privacy (which is often applied by racialized people) is largely overlooked in favour of an individualistic approach. As noted in *Cross-Cultural Privacy Differences*, individuals from collectivistic cultures

[4] Xingyu Chen et al, "Exploring racial and gender disparities in voice biometrics" (2022) 12:1 Scientific Reports 3723.
[5] Statistics Canada, "Racialized Canadians are less likely to find as good jobs as their non-racialized and non-Indigenous counterparts early in their careers" (18 January 2023), online: <www150.statcan.gc.ca/n1/daily-quotidien/230118/dq230118b-eng.htm>; Annette Bernhardt, Lisa Kresge & Reem Suleiman, "The Data-Driven Workplace and the Case for Worker Technology Rights" (2023) 76:1 ILR Rev 3 at 11-13.

contextualize themselves as part of a group and are therefore concerned with privacy protection of the group.[6] Threats to privacy affect individuals as well as their groups, especially in the context of modern technology, which has caused everyone and everything to be connected.[7] The concept of collectivism could be incorporated into privacy guidance documents, while maintaining individualistic rights, to ensure that often overlooked and/or minority perspectives on privacy are considered in Canadian guidance and policy.

LGBTQ2SIA+ Considerations

There are pre-existing privacy concerns regarding biometric data collection among gender and sexual minorities.[8] Key concerns for these communities include sexual interest disclosures for LGBTQ2SIA+ individuals and identity verification systems that employ facial recognition algorithms. The importance of protecting the privacy rights of LGBTQ2SIA+ individuals in relation to current biometric technologies is heightened in the context of the well-documented history of the Canadian state's concerted efforts to develop and use surveillance technologies to identify, target, and discriminate against gender and sexual minorities.[9] Further, protection of LGBTQ2SIA+ individuals against involuntary public disclosure is especially urgent considering the escalating sentiments of transphobia in Canada towards children and minors, which has been largely couched in the language of parental rights.[10]

Facial recognition technology, a form of biometric data collection, is now able to detect sexual orientation with a significantly higher accuracy rate than humans, potentially leading to the public disclosure of individuals' sexual orientation without their consent.[11] Such disclosures can also happen through data breaches about sexual interests.[12] Unwanted sexual interest disclosures can compromise individuals' safety or dignity, especially in

---

[6] Yao Li, "Cross-Cultural Privacy Differences" in Bart P. Knijnenburg et al, eds, *Modern Socio-Technical Perspectives* (Cham, Switzerland: Springer, 2022) 267 at 278-79.
[7] Karanja, *supra* note 2 at 6.
[8] Shruti Sannon & Andrea Forte, "Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next" (2022) 6:CSCW2 Proceedings of the ACM on Human-Computer Interaction at 16.
[9] Gary Kinsman, ""Character Weaknesses" and "Fruit Machines": Towards an Analysis of the Anti-Homosexual Security Campaign in the Canadian Civil Service" (1995) 35 Labour / Le Travail 133.
[10] Jenna Benchetrit, "How the parental rights movement resurged in response to trans inclusivity in classrooms" *CBC News* (8 April 2023), online: <cbc.ca/news/world/parental-rights-movement-us-canada-1.6796070>.
[11] Phillip H.C. Wilkinson, "The Legal Implications of Sexual Orientation-Detecting Facial Recognition Technology" (2021) 20 The Dukeminier Awards 301 at 301, 305.
[12] Sannon & Forte, *supra* note 8 at 11.

consideration of homophobic sentiments within society.[13] Furthermore, the disclosure of one individual's sexual orientation can impact and put at equal risk others within their network such as their children, partners, and former partners.[14] Similar to how racialized peoples take a collectivistic approach to privacy, the protection of LGBTQ2SIA+ individuals' privacy must therefore be instituted with an eye to the collective of which they are part.

Biometric facial recognition, matched with an individual's government-issued identity documents, has also become increasingly relied upon as a line of defense in identity verification.[15] Automatic Gender Recognition as a subfield of facial recognition is designed to identify individuals' gender from photos or videos, with proposed applications in physical access control, data analytics, and advertising.[16] The issue with this use of biometrics is that their facial recognition algorithms are typically trained on data sets that sort individuals into a gender binary of male or female; consequently, trans individuals face higher risk of being misgendered or misidentified, restricting their access to certain products, services and spaces or resulting in issues with the government or police.[17] For example, 71.7% of non-binary people reported in a 2020 survey that they had no identity documents with their preferred gender marker.[18] Without formal documents that correctly identify their gender, non-binary people therefore have little power to combat the false identifications made by cis-normative algorithms. Additionally, the privacy rights of trans individuals require that the algorithms underlying biometrics, if used in identity verification, be trans-inclusive.

The benefits of biometrics are often accompanied by risks and can be used in ways that are overly invasive; one notable example is menstrual cycle tracking applications. Many applications have become increasingly advanced over time through the collection of more types of and more detailed biometric data. For example, several menstrual cycle tracking applications have become more accurate in their predictions by collecting detailed and varied types of biometric data such as body temperature,

---

[13] Wilkinson, *supra* note 11 at 342.
[14] Sannon & Forte, *supra* note 8 at 20.
[15] Os Keyes, "The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition" (2018) 2:CSCW Proceedings of the ACM on Human-Computer Interaction.
[16] *Ibid.*
[17] *Ibid.*
[18] Trans PULSE Canada, *Non-Binary People and Identity Documents: A report prepared for the Saskatchewan Human Rights Commission* (London, Ontario: Trans PULSE Canada, 2020).

sleep patterns, and heart rate data.[19] It is important for private organizations to be cognizant that, despite trying to provide the best product through biometric processing, the use and retention of these types of biometric data creates serious risk of harm to women and transgender people. The lack of specific guidance on this issue only exacerbates the possibility that organizations will employ biometric processing in a way that may cause harm. Although products such as menstrual cycle tracking or DNA analysis services are helpful to consumers, the organizations providing these services must be aware of the possible risks.

Indigenous Considerations

Biometric processing technologies may significantly exacerbate privacy concerns held by Indigenous peoples in Canada, including fears of targeting through surveillance, which could undermine Indigenous data sovereignty.[20]

The overincarceration of Indigenous people in Canada is an ongoing crisis.[21] Militarized police responses to Indigenous protests, such as the Oka Crisis and Wet'suwet'en Blockade, are part of recent Canadian history.[22] The RCMP has unlawfully used facial recognition technology to identify individuals,[23] and these technologies "may inspire a false confidence in the identification of individuals believed to have committed crimes."[24] "When governments emphasize truth and reconciliation while their agencies employ technology to surveil Indigenous individuals and communities, it negatively impacts a historically tense relationship."[25]

OPC guidance on biometric processing technologies should strongly recommend proactive measures to prevent their use as a weapon of

---

[19] Andrea Ford, Giulia De Togni & Livia Miller, "Hormonal Health: Period Tracking Apps, Wellness, and Self-Management in the Era of Surveillance Capitalism" (2021) 7:1 Engaging Science, Technology, and Society 48; Elisabet Alzueta et al, "Tracking Sleep, Temperature, Heart Rate, and Daily Symptoms Across the Menstrual Cycle with the Oura Ring in Healthy Women" (2022) 14 Int J Womens Health 491.
[20] Goltz et al, "Biometrics and Facial Recognition" in *Real World AI Ethics for Data Scientists: Practical Case Studies* (Boca Raton: CRC Press, 2023) at 72-73.
[21] Scott Clark, *Overrepresentation of Indigenous People in the Canadian Criminal Justice System: Causes and Response* (Ottawa: Research and Statistics Division, Department of Justice Canada, 2019).
[22] Goltz et al, *supra* note 20 at 72.
[23] Office of the Privacy Commissioner of Canada, *Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology* (Quebec: Office of the Privacy Commissioner of Canada, 2021).
[24] Goltz et al, *supra* note 20 at 73.
[25] *Ibid.*

colonial violence. For example, the OPC can affirm that these technologies, when used to collect Indigenous data, should be governed according to Indigenous laws and values, including Indigenous data sovereignty.[26] Indigenous data sovereignty is a key aspect of the right to self-determination as unequivocally affirmed in the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP).[27] Canadian legal frameworks affirming Indigenous data sovereignty should adhere to the principles of OCAP™: that First Nations must maintain Ownership, Control, Access, and Possession of and to their data.[28]

In their recent scholarship on the ethics of biometrics, Joey Miller and Andrea Sullivan-Clarke wrote that "[a] policy developed solely from a Western worldview will lack the resources to mitigate oppression because it considers the technology a tool and not worthy of standing in relation to it. Collaborating with local Indigenous communities and applying Indigenous values by asking how the technology contributes to harmony or whether it introduces chaos, would not only strengthen relations between nations, but it would also provide a more robust understanding of the technology."[29] Public and private actors must carefully consider Indigenous laws, values, and lived experiences, the long history of abuse of Indigenous data,[30] and their relationships with Indigenous communities when using biometric processing technologies.

---

[26] John Borrows & Lisa Austin, "The Digital Charter Implementation Act ignores Indigenous Data Sovereignty", *Schwartz Reisman Institute for Technology and Society* (6 December 2022), online: <srinstitute.utoronto.ca/news/digital-charter-implementation-act-ignores-indigenous-data-sovereignty>.
[27] Chidi Oguamanam, *Indigenous Data Sovereignty, Retooling Indigenous Resurgence for Development, Centre for International Governance Innovation* (Waterloo: CIGI Papers Series, 2019) at 8.
[28] First Nations Information Governance Centre, *Ownership, Control, Access and Possession (OCAP™): The Path to First Nations Information Governance* (Ottawa: First Nations Information Governance Centre, 2014).
[29] Goltz et al, *supra* note 20 at 73.
[30] First Nations Information Governance Centre, *supra* note 28 at 8-10.

BC FIPA Suggestions

As mentioned in the introduction to this submission, our suggestions are intended to apply to both the public institution and private organization guidance documents. Further, the following suggestions stem from the perspectives we have focused on, but in practice should encapsulate all marginalized perspectives.

1. Perspectives

Include guidance that reminds public institutions and private organizations to consider the marginalized perspectives they serve and their employees.

First and foremost, the guidance documents should provide reminders and examples of how marginalized groups can be considered in either the private or public context. Regardless of whether organizations are aware of marginalized vulnerabilities, or the bias embedded in technology, these organizations should be called to consider these factors by the guidance.

Additionally, the guidance documents should describe the seriousness of using biometric data and the potential harmful consequences at their onsets.

2. Consultation

Include examples for how public institutions and private organizations can practice the protection of marginalized perspectives.

Some examples include providing greater control over information, facilitating privacy decisions, and creating privacy systems to protect information. These examples should be considered by public institutions and private organizations at all stages of data collection—including prior to data being collected, such as hiring processes. Additionally, all these examples can be actualized through greater public institution and private organization transparency regarding how biometric data is being collected, used, or shared.

3. Examples

Improvements to general clarity through additional description and examples.

Overall, BC FIPA noted that the clarity of the guidance documents could be improved through additional description or examples. One instance is the

general definition of biometric, which lacks description and sufficient examples, as biometric information varies widely. Although succinct writing is effective, a balance should be met between concision and providing sufficient information to ensure the guidance is clear for the broad intended audience of these guidance documents.

OPC Biometric Definition	BC FIPA Biometric Definition (Example)
"Biometrics" refers to the quantification of human characteristics into measurable terms. They are used for recognition and, less commonly, for categorization.	Biometric information is generally electronically stored information based on physical characteristics such as fingerprints, voiceprints, retinal scans, hand geometry or DNA. Biometrics is generally not a one-to-one copy of your characteristic as scans are turned into a formula and the scan is deleted.

OPC Biometric Overview	BC FIPA Biometric Overview (Example)
There are three main categories used for recognition: • Morphological biometrics — such as fingerprints; • Behavioural biometrics — such as keystroke patterns; and • Biological biometrics — such as DNA.	There are three main categories used for recognition: • Morphological biometrics — such as fingerprints, eye scans, and facial recognition; • Behavioural biometrics — such as keystroke patterns, mouse clicks, and motor skills; and • Biological biometrics — such as DNA or blood. Biometric information is often used in the workplace to allow an individual entry into something, such as an electronic device or the workplace itself. Additionally, biometrics can also be used to track employees based on arrival, departure, and break times. Biometrics is considered a highly secure and specific method of identifying people because the data is tied to one individual. However, the use of biometrics comes with increased risk and need for data security.

Another example is the lack of clarity as to whether biometric data is considered personal information; for example, if information continues to be personal information even after being formulaically processed, and whether the same rules governing personal information apply to biometric data. Further, if biometric data is personal information, then this point should be stressed to both public institutions and private organizations.

Conclusion

It is widely acknowledged that technology, privacy, and access to information mechanisms are not designed with marginalized populations in mind. As such, it is up to regulators to fill this gap. The equal protection of the privacy of Canadians requires regulators to consider the social distribution of privacy policy and its effects, especially for marginalized groups. Charles D. Raab articulates this consideration, "do women experience more privacy invasions and benefit less from data protection law than men; non-whites than whites; poor than rich; old than young; ill people than healthy; and so on?"[31]

Consequently, the ability for privacy laws to operate equitably and to protect all Canadians is dependent on the ability of regulators to consider the needs of vulnerable populations.

BC FIPA thanks the OPC for their consideration of our submission and looks forward to the amendments made to the biometric processing guidance documents.

[31] Karanja, *supra* note 2 at 8.